# 国家信息安全漏洞共享平台(CNVD)

# 信息安全漏洞周报

**2018 年 4 月 09 日-2018 年 4 月 15 日** **2018 年第 15 期**

## 本周漏洞态势研判情况

本周信息安全漏洞威胁整体评价级别为**中**。

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 316 个，其中高危漏洞 113 个、中危漏洞 188 个、低危漏洞 15 个。漏洞平均分值为 5.96。本周收录的漏洞中，涉及 0day 漏洞 80 个（占 25%），其中互联网上出现“Tenda AC15 Router 远程代码执行漏洞、WordPress Ajax Pagination（twitter Style）插件路径遍历漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 581 个，与上周（562 个）环比增长 3%。

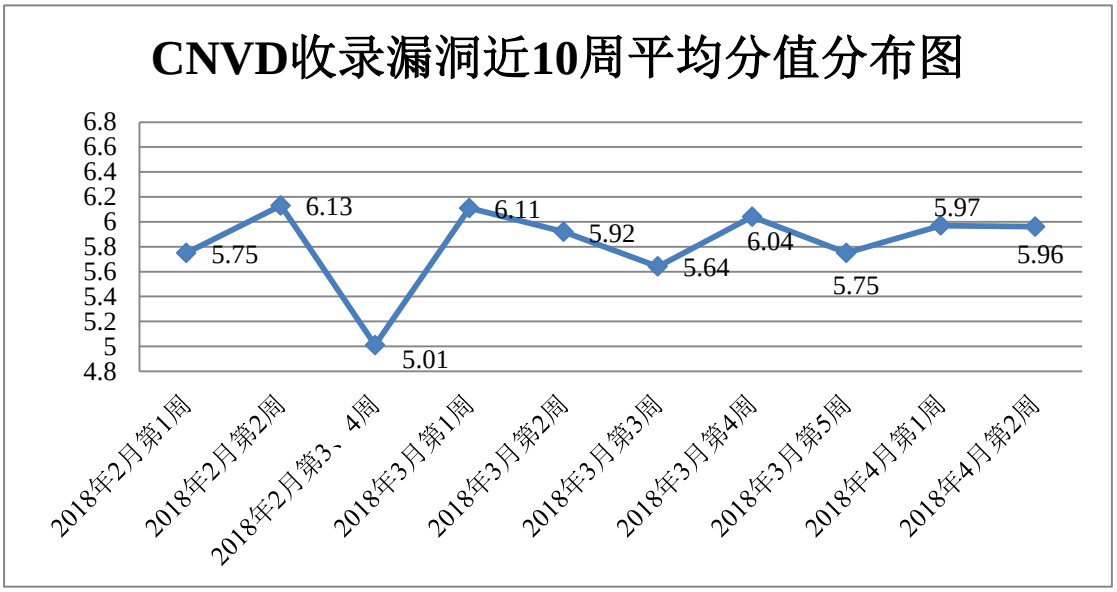


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京天融信网络安全技术有限公司、哈尔滨安天科技股份有限公司、华为技术有限公司、北京神州绿盟科技有限公司、北恒安嘉新(北京)

科技股份公司等单位报送公开收集的漏洞数量较多。四川虹微技术有限公司（子午攻防实验室）、中新网络信息安全股份有限公司、山石网科通信技术有限公司、上海观安信息技术股份有限公司、安徽三实信息技术服务有限公司、福建省海峡信息技术有限公司、安徽锋刃信息科技有限公司及其他个人白帽子向 CNVD 提交了 581 个以事件型漏洞为主的原创漏洞，其中包括 360 网神（补天平台）和漏洞盒子向 CNVD 共享的白帽子报送的 335 条原创漏洞信息。

表 1 漏洞报送情况统计表

| 报送单位或个人 | 漏洞报送数量 | 原创漏洞数量 |
|---|---|---|
| 北京天融信网络安全技术有限公司 | 244 | 11 |
| 漏洞盒子 | 226 | 226 |
| 哈尔滨安天科技股份有限公司 | 203 | 0 |
| 360 网神（补天平台） | 109 | 109 |
| 华为技术有限公司 | 147 | 0 |
| 北京神州绿盟科技有限公司 | 71 | 0 |
| 恒安嘉新(北京)科技股份公司 | 67 | 0 |
| 中国电信集团系统集成有限责任公司 | 65 | 0 |
| 新华三技术有限公司 | 45 | 0 |
| 北京无声信息技术有限公司 | 12 | 0 |
| 北京知道创宇信息技术有限公司 | 4 | 0 |
| 四川虹微技术有限公司（子午攻防实验室） | 18 | 18 |
| 中新网络信息安全股份有限公司 | 11 | 11 |
| 山石网科通信技术有限公司 | 8 | 8 |
| 上海观安信息技术股份有限公司 | 6 | 6 |
| 安徽三实信息技术服务有限公司 | 3 | 3 |
| 福建省海峡信息技术有限公司 | 2 | 2 |

| | | |
|---|---|---|
| 安徽锋刃信息科技有限公司 | 1 | 1 |
| CNCERT 吉林分中心 | 3 | 3 |
| CNCERT 贵州分中心 | 1 | 1 |
| CNCERT 广东分中心 | 1 | 1 |
| CNCERT 宁夏分中心 | 1 | 1 |
| 个人 | 180 | 180 |
| 报送总计 | 1428 | 581 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 316 个漏洞。其中应用程序漏洞 166 个，操作系统漏洞 60 个，WEB 应用漏洞 66 个，安全产品漏洞 9 个，网络设备漏洞 9 个，数据库漏洞 6 个。

表 2 漏洞按影响类型统计表

| 漏洞影响对象类型 | 漏洞数量 |
|---|---|
| 应用程序漏洞 | 166 |
| 操作系统漏洞 | 60 |
| WEB 应用漏洞 | 66 |
| 安全产品漏洞 | 9 |
| 网络设备漏洞 | 9 |
| 数据库漏洞 | 6 |

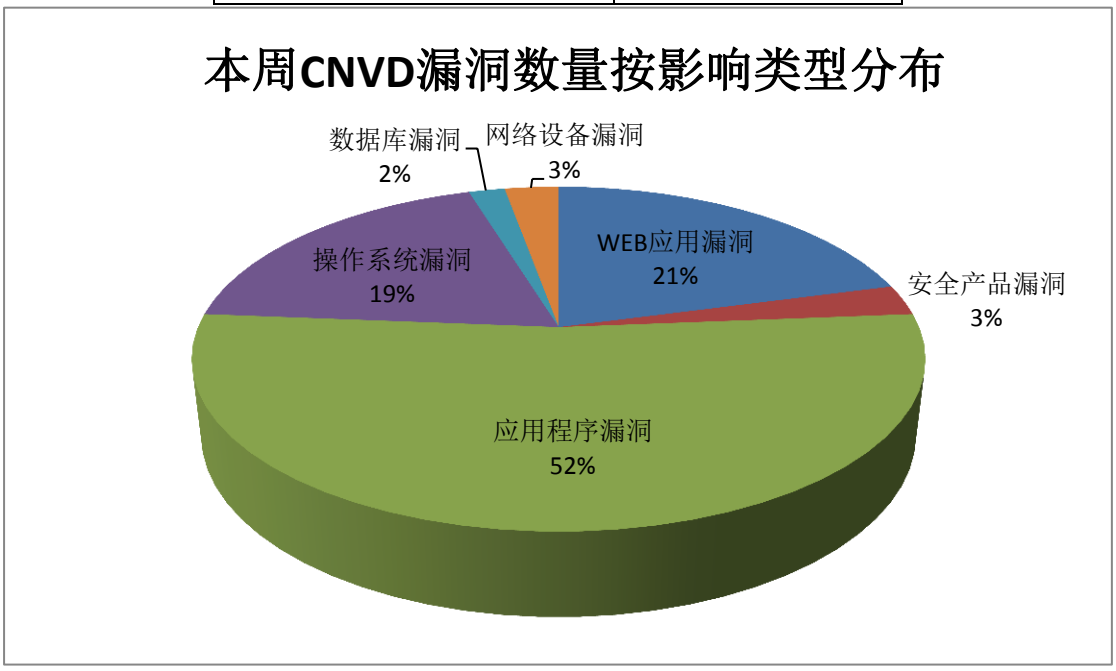

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Apple、Cisco、Google 等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

表 3 漏洞产品涉及厂商分布统计表

| 序号 | 厂商（产品） | 漏洞数量 | 所占比例 |
|---|---|---|---|
| 1 | Apple | 18 | 6% |
| 2 | Cisco | 17 | 4% |
| 3 | Google | 12 | 4% |
| 4 | IBM | 11 | 3% |
| 5 | Microsoft | 10 | 3% |
| 6 | Apache | 9 | 3% |
| 7 | Dell | 9 | 3% |
| 8 | Pivotal Software | 9 | 3% |
| 9 | McAfee | 8 | % |
| 10 | 其他 | 213 | 67% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 7 个电信行业漏洞，30 个移动互联网行业漏洞，6 个工控行业漏洞（如下图所示）。其中，“Cisco Smart Install 未授权访问漏洞、多款 Apple 产品 CoreFoundation 竞争条件漏洞、Google Android System 权限提升漏洞（CNVD-2018-07452）、Moxa Mxview 信息泄露漏洞、多款 Apple 产品 WebKit 内存破坏漏洞（CNVD-2018-07643）”的综合评级为“高危”。相关厂商已经发布了上述漏洞的修补程序，请参照 CNVD 相关行业漏洞库链接。

电信行业漏洞链接：http://telecom.cnvd.org.cn/

移动互联网行业漏洞链接：http://mi.cnvd.org.cn/

工控系统行业漏洞链接：http://ics.cnvd.org.cn/

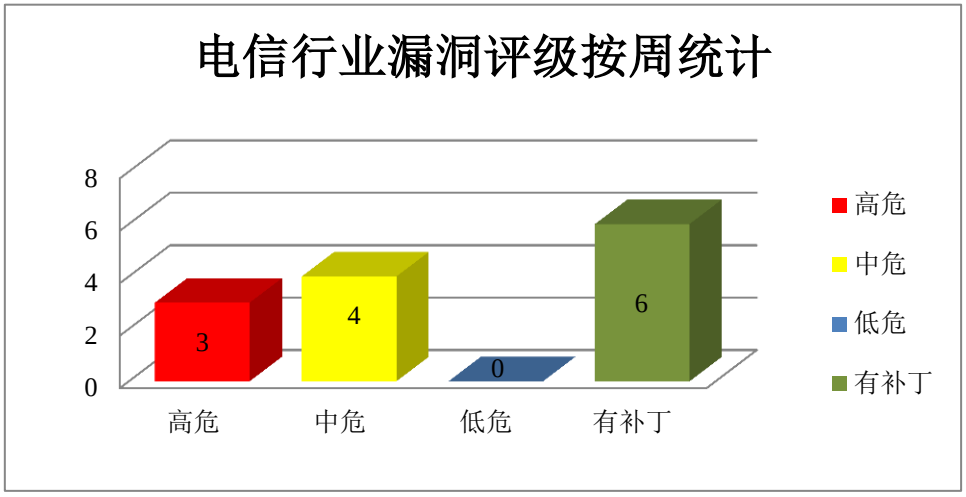


图 3 电信行业漏洞统计

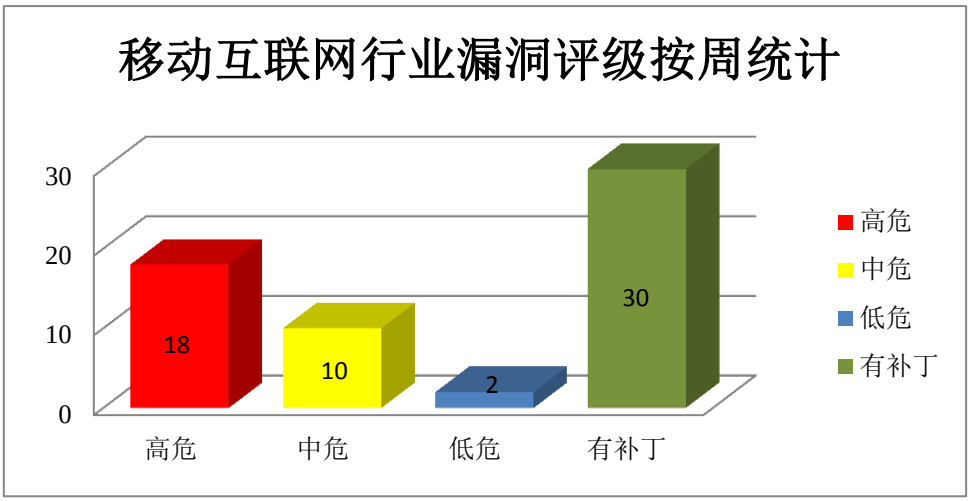


图 4 移动互联网行业漏洞统计

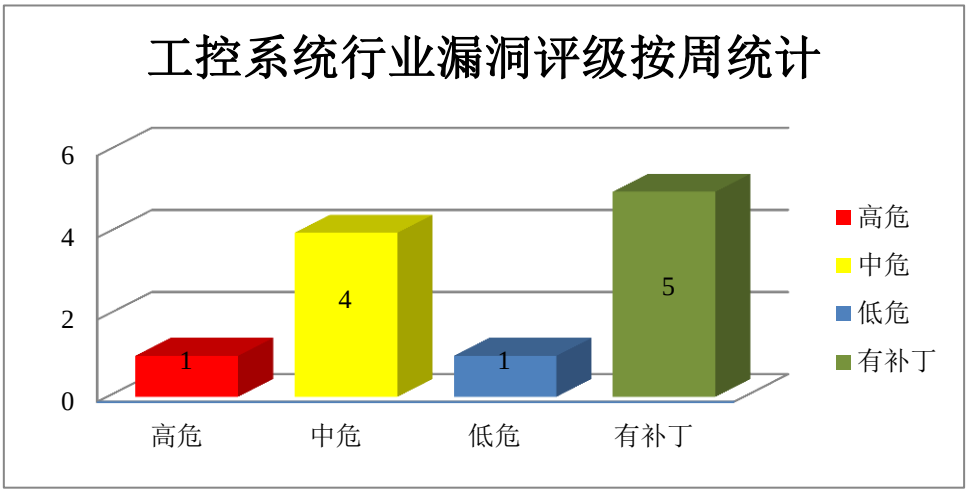


图 5 工控行业漏洞统计

## 本周重要漏洞安全告警

本周，CNVD 整理和发布以下重要安全漏洞信息。

## 1、Microsoft 产品安全漏洞

Microsoft Windows 10 和 Windows Server 2016 等都是美国微软（Microsoft）公司的一系列操作系统。Microsoft Windows Installer 是一款 Windows 应用程序的安装和配置服务。Microsoft Malware Protection Engine 是恶意程序保护引擎。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限或执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Desktop Bridge VFS 权限提升漏洞、Microsoft Edge scripting 引擎内存破坏漏洞（CNVD-2018-07281）、Microsoft Internet Explorer 内存破坏漏洞（CNVD-2018-07279、CNVD-2018-07326）、Microsoft Malware Protection Engine 远程代码执行漏洞（CNVD-2018-07296）、Microsoft Windows GDI 权限提升漏洞（CNVD-2018-07324、CNVD-2018-07325）、Microsoft Windows Installer 权限提升漏洞。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-07322

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07281

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07279

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07326

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07296

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07324

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07325

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07323

## 2、Apple 产品安全漏洞

Apple iOS 是为移动设备所开发的一套操作系统；Safari 是一款 Web 浏览器，是 Mac OS X 和 iOS 操作系统附带的默认浏览器。iCloud for Windows 是一款基于 Windows 平台的云服务。WebKit 是其中的一个 Web 浏览器引擎组件。本周，上述产品被披露存在内存破坏漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：多款 Apple 产品 WebKit 内存破坏漏洞（CNVD-2018-07632、CNVD-2018-07633、CNVD-2018-07634、CNVD-2018-07635、CNVD-2018-07643、CNVD-2018-07644、CNVD-2018-07645、CNVD-2018-07646）。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-07632

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07633

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07634

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07635

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07643

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07644

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07645

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07646

### 3、Google 产品安全漏洞

Android 是美国谷歌公司和开放手持设备联盟共同开发的一套以 Linux 为基础的开源操作系统。Google Chrome 是一款 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏提升权限或执行任意代码等。

CNVD 收录的相关漏洞包括：Google Android System 权限提升漏洞（CNVD-2018-07447、CNVD-2018-07448、CNVD-2018-07452）、Google Android System 远程代码执行漏洞（CNVD-2018-07446、CNVD-2018-07449、CNVD-2018-07453、CNVD-2018-07666）、Google Chrome interstitials 命令执行漏洞。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-07447

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07448

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07452

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07446

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07449

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07453

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07666

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07437

### 4、Cisco 产品安全漏洞

Cisco IOS Software 和 IOS XE Software 都是美国思科（Cisco）公司为其网络设备开发的操作系统。本周，该产品被披露存在拒绝服务和越权访问漏洞，攻击者可利用漏洞发起拒绝服务攻击或以特权登录设备。

CNVD 收录的相关漏洞包括：Cisco IOS Software 和 IOS XE Software 拒绝服务漏洞、Cisco IOS Software 和 IOS XE Software 拒绝服务漏洞（CNVD-2018-07300、CNVD-2018-07302、CNVD-2018-07314）、Cisco IOS XE Software 拒绝服务漏洞（CNVD-2018-07303、CNVD-2018-07304、CNVD-2018-07318）、Cisco IOS XE Software 越权访问漏洞。除“Cisco IOS Software 和 IOS XE Software 拒绝服务漏洞（CNVD-2018-07314）、Cisco IOS XE Software 拒绝服务漏洞（CNVD-2018-07303）”外，其余漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-07319

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07300

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07302

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07314

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07303

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07304

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07318

http://www.cnvd.org.cn/flaw/show/CNVD-2018-07315

### 5、WordPress Ajax Pagination（twitter Style）插件路径遍历漏洞

WordPress 是 WordPress 软件基金会的一套使用 PHP 语言开发的博客平台。本周，WordPress 被披露存在路径遍历漏洞，远程攻击者可借助‘loop’参数中的‘..’序列利用该漏洞读取任意文件。目前，厂商尚未发布漏洞修补程序。CNVD 提醒广大用户随时关注厂商主页，以获取最新版本。参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-07478

更多高危漏洞如表 4 所示，详细信息可根据 CNVD 编号，在 CNVD 官网进行查询。参考链接：http://www.cnvd.org.cn/flaw/list.htm

表 4 部分重要高危漏洞列表

| CNVD 编号 | 漏洞名称 | 综合评级 | 修复方式 |
|---|---|---|---|
| CNVD-2018-07293 | beep 本地权限提升漏洞 | 高 | 厂商已发布漏洞修复程序，请及时关注更新：https://security-tracker.debian.org/tracker/CVE-2018-0492 |
| CNVD-2018-07295 | Spring Framework spring-messaging 模块存在远程代码执行漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://pivotal.io/security/cve-2018-1270 |
| CNVD-2018-07298 | Moxa Mxview 信息泄露漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.moxa.com/ |
| CNVD-2018-07456 | F5 BIG-IP 任意代码执行漏洞（CNVD-2018-07456） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://support.f5.com/csp/article/K11718033 |
| CNVD-2018-07458 | Pivotal Garden 信息泄露漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://pivotal.io/security/cve-2015-5350 |
| CNVD-2018-07463 | SchedMD Slurm SQL 注入漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接:https://www.schedmd.com/news.php?id=201 |

| | | | |
|---|---|---|---|
| CNVD-2018-07475 | Pivotal Spring Boot 权限提升漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://pivotal.io/security/cve-2018-1196 |
| CNVD-2018-07481 | Wicket jQuery UI WYSIWYG 编辑器漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：http://www.7thweb.net/wicket-jquery-ui |
| CNVD-2018-07557 | Apple MACOS/OSX 任意代码执行漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://support.apple.com/en-us/HT208692 |
| CNVD-2018-07592 | Parsec 访问限制绕过漏洞 | 高 | 厂商已发布漏洞修复程序，请及时关注更新：https://github.com/chrisd1100/uncurl/releases/tag/0.07 |

小结：本周，Microsoft 被披露存在多个漏洞，攻击者可利用漏洞提升权限或执行任意代码。此外，Google、Apple、Cisco 等多款产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码、提升权限或发起拒绝服务攻击等。另外，WordPress 被披露存在路径遍历漏洞，远程攻击者可借助‘loop’参数中的‘..’序列利用该漏洞读取任意文件。建议相关用户随时关注上述厂商主页，及时获取修复补丁或解决方案。

## 本周漏洞要闻速递

### 1. 施耐德电气修补 16 个 U.motion Builder 软件漏洞

施耐德电气于上周向其客户通报说已修复 U.motion Builder 最新版本中的 16 个漏洞，其中包括那些被评为严重和高危的漏洞，例如可能导致信息泄露的路径遍历或者其他一些错误，以及通过 SQL 注入造成的远程代码执行缺陷。最严重漏洞（CVE-2017-7494）的 CVSS 评分达到了 10，根据介绍，该漏洞允许远程执行代码，对 Samba 软件套件造成了一定影响。这些问题影响到 U.motion Builder 1.3.4 之前的版本。目前施耐德除了提供补丁之外，还分享了一些缓解潜在攻击的建议。

参考链接：https://www.easyaq.com/news/549041533.shtml

### 2. Linux Beep 曝提权漏洞，黑客可窥探用户敏感文件

安全研究人员近日指出，Dediban 和 Ubuntu（开源 GNU/Linux 操作系统） 发行版中预装的 Beep 软件包存在漏洞 CVE-2018-0492，允许攻击者探测设备中的敏感文件，包括 Root 用户的文件。此外，该漏洞还允许本地提权，进而完全访问设备。该漏洞目前已在 Debian 和 Ubuntu 较新的版本中得到修复。

参考链接：https://www.easyaq.com/news/610364632.shtml

## 关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

## 关于 CNCERT

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82991537